УДК 347

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УГОЛОВНОМ ЗАКОНОДАТЕЛЬСТВЕ ЗАРУБЕЖНЫХ ГОСУДАРСТВ

Челмодеева И.О.
Адъюнкт
Академии МВД ДНР имени Ф.Э. Дзержинского

Аннотация: В статье рассмотрены вопросы обеспечения информационной безопасности в уголовном законодательстве зарубежных государств, проведен его сравнительный анализ **с** целью совершенствования отечественного законодательства на основе учета и заимствования положительного зарубежного опыта.

Ключевые слова: информационная безопасность; кибербезопасность; шпионаж; уголовно-правовая охрана информационной безопасности; компьютерные преступления.

ENSURING INFORMATION SECURITY IN THE CRIMINAL LEGISLATION OF FOREIGN STATES

Chelmodeeva I.O.

Annotation: The article defines the features of ensuring information security in the criminal legislation of foreign states, its comparative analysis was carried out in order to improve domestic legislation on the basis of taking into account and borrowing foreign experience.

Key words: information security; cybersecurity; espionage; criminal information security; computer crimes.

Становление правового регулирования сферы информационной безопасности началось в конце XX века. Это связано с осознанием угроз, возникающих в связи с развитием информационных технологий, социально-экономических, военных и политических последствий последней информационной революции в странах, которые первыми начали активную трансформацию в направлении построения информационного общества. В связи с этим актуальными становятся вопросы обеспечения информационной безопасности.

Для Донецкой Народной Республики вопрос обеспечения информационной безопасности приобретает особенно важное значение в сложившихся общественно-политических условиях. Это невозможно обеспечить без основательной теоретической основы, научно-экспертной деятельности, изучения и внедрения лучшего из соответствующего зарубежного опыта.

Анализ законодательных актов зарубежных государств свидетельствует о том, что информационная и сетевая безопасность понимается в большинстве государств

как способность сети или системы противостоять злонамеренным действиям, которые могут нарушить доступность, целостность и конфиденциальность информации, которая хранится или передается, а также услуг, предоставляемых посредством сети или информационной системы. Соблюдение безопасности определяется как доступность, идентификация, целостность, конфиденциальность информации. Особое внимание при этом уделяется законодательной базе, которая охватывает вопросы перехвата и дешифровки информации [1, с. 8].

При этом выбор направлений политики обеспечения информационной безопасности и форм их закрепления в национальных правовых системах существенно отличается и обусловлен рядом исторических, культурных, правовых и экономических факторов.

Уголовное законодательство зарубежных стран характеризуется преимущественно отсутствием системного подхода к уголовно-правовой охране информационной безопасности [2, с. 131]. В качестве родового или видового объекта преступления информационная безопасность, как правило, не выделяется. Исключением является УК Польши, предусматривающая в статья 265-269 главы XXXIII преступления против охраны информации [3, с. 200-201].

В некоторых зарубежных странах, преступления против информационной безопасности иногда установлены отдельной главой уголовного закона, однако они включают в себя уголовно-правовые нормы, предусматривающие ответственность за преступления против безопасного использования информационно-телекоммуникационных технологий. При этом они либо выделяются в самостоятельный раздел или главу, либо рассредоточены по различным разделам или главам.

Во всех без исключения странах Европейского союза вопросам правового обеспечения информационной безопасности уделяется особое внимание. При этом первостепенное значение приобретают вопросы противодействия киберугрозам, которые являются составляющими процесса обеспечения информационной безопасности. С 1999 года реализуются программы «Безопасный Интернет» (Safer Internet), в рамках которых осуществляются мероприятия, направленные на борьбу не только с вредным контентом, но и с опасным поведением в сети.

В Австрии, Финляндии и Ирландии, как и в других странах ЕС, значительное внимание уделяется проблемам кибербезопасности, очерченным в документе Европейской комиссии «На пути к общей политики в сфере борьбы с киберпреступностью», где последняя определяется как уголовные действия, совершенные с использованием электронных коммуникационных сетей и информационных систем или против таких сетей и систем [4, с. 82-83].

В Беларуси отсутствуют специальные законы о киберпреступности, но некоторые аспекты урегулированы Уголовным кодексом и нормативными актами, регулирующими интернет. Серьезной проблемой в Беларуси является создание и распространение порнографии, включая детскую порнографию, особенно учитывая тенденцию быстрого распространения информации в соцсетях [5, с. 182].

Защита информации от неправомерного доступа тесно связана с категорией «тайна», в связи с чем важным является исследование вопросов криминализации данного преступления в зарубежных странах.

Общественные отношения, возникающие в сфере оборота информации с ограниченным доступом в зарубежных странах, охраняются отдельными уголовно-правовыми нормами. Анализ законодательства зарубежных стран, которое предусматривает уголовную ответственность за указанные посягательства, дает основания считать, что преступления, предметом которых является информация с ограниченным доступом, в зависимости от владельца информации можно разделить на две группы. К первой группе следует отнести преступления, предметом которых признается информация, являющаяся собственностью государства. Вторую группу составят преступления, предметом которых выступает информация, являющаяся собственностью физических и негосударственных юридических лиц.

К первой группе преступлений можно отнести шпионаж, разглашение государственной тайны, разглашение служебной тайны, содержащиеся в уголовных кодексах подавляющего большинства стран. Особенностью шпионажа в законодательствах зарубежных стран является то, что, во-первых, адресатом передачи информации являются иностранные государства, иностранные организации или их представители; во-вторых, субъектом этого преступления признается иностранный гражданин или лицо без гражданства; в-третьих, сведения могут быть использованы для нанесения вреда суверенитету, территориальной целостности или внешней безопасности страны. Предметом шпионажа законодательства указанных стран признают государственную информацию [6, с. 227].

Особого внимания требуют преступления, предметом которых признаются сведения, являющиеся собственностью государства, но не составляющие государственной тайны. В законодательствах разных стран это понятие терминологически имеет разные названия: «официальные акции или сведения» (США), «сведения, не подлежащие оглашению» (Латвия), «информация для внутреннего пользования» (Эстония), «конфиденциальная информация» (Дания), «служебная тайна» (Республика Беларусь, Республика Болгария, Республика Польша, Швейцарская Конфедерация) и другие.

Следует отметить, что информация с ограниченным доступом, которая является собственностью государства, но не составляет государственной тайны, в одних странах охраняется отдельными уголовно-правовыми средствами, а в других – наряду с государственной и другими видами тайн [2, с. 99-100].

Изучение практики зарубежных стран в построении собственных моделей правового обеспечения информационной безопасности, противодействии киберугрозам позволяет резюмировать об отсутствии единой модели национальной системы обеспечения информационной безопасности уголовно-правовыми средствами. Вопросы уголовно-правовой охраны информации и информационной безопасности разрешаются различным способом. При этом системный подход в данном вопросе отсутствует во всех странах, кроме Польши.

Преступления против информационной безопасности расположены в различных разделах и главах Особенной части уголовного закона зарубежных стран. Преступления, посягающие на компьютерную информацию, как правило, объединены в один раздел или главу. Зарубежные законодатели уделяют повышенное внимание к уголовно-правовой охране государственных информационных ресурсов, что определяется в установлении ответственности за посягательство на них не в общих, а в специальных нормах.

Приоритетным направлением является совершенствование законодательства, устанавливающего ответственность за правонарушения, разработка и законодательное закрепление в одном перечня правонарушений и видов ответственности в сфере информационной безопасности. То есть необходимо закрепить преступления против информационной безопасности в отдельной главе уголовного закона.

Список литературы:

1. Информационная безопасность: учебное пособие / В.Н. Ясенев, А.В. Дорожкин, А.Л. Сочков, О.В. Ясенев. Под общей редакцией В.Н. Ясенева. – Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. – 198 с.
2. Ефремова М.А. Уголовно-правовая охрана информационной безопасности: дис. ... докт. юрид. наук 12.00.08 / М.А. Ефремова. – Москва, 2017. – 427 с.
3. Уголовный кодекс Республики Польша / под общ. ред. Н.Ф. Кузнецовой. – Санкт-Петербург: Юридический центр Пресс, 2001. – 234 с.
4. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – Москва: ООО «Юрлитинформ», 2001. – 496 с.
5. Дубко М.А. Международное сотрудничество в сфере уголовно-правовой борьбы с неправомерным завладением компьютерной информацией / М.А. Дубко // Вестник Полоцкого государственного университета. Сер. D, Экономические и юридические науки: научно-теоретический журнал. – Новополоцк: ПГУ, 2012. – № 14. – С. 180-183.
6. Азаров Д.С. Злочини у сфері комп’ютерної інформації (кримінально-правове дослідження) / Д.С. Азаров. – Київ: Атіка, 2007. – 304 с.